UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/087,779	03/05/2002	Thomas L. Johnson	1875.2050000	8819

			EXAMINER
26111 7590 01/17/2007			
STERNE, KESSLER, GOLDSTEIN & FOX PLLC			SEFCHECK, GREGORY B
1100 NEW YORK AVENUE, N.W.			
WASHINGTON, DC 20005		ART UNIT	PAPER NUMBER
		2616	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	01/17/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 01/17/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

fadkt@skgf.com

PTOL-90A (Rev. 10/06)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _15 November 2006_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-39_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-39_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

- Applicant's Pre-Appeal Conference Request filed 11/15/2006 is

  acknowledged.

- In view of the required new rejections below, prosecution has been

  reopened.

- Claims 1-39 remain pending.

Claim Rejections - 35 USC § 101

1.   35 U.S.C. 101 reads as follows:

   Whoever invents or discovers any new and useful process, machine, manufacture, or
   composition of matter, or any new and useful improvement thereof, may obtain a patent
   therefor, subject to the conditions and requirements of this title.

2.   Claims 1-26 are rejected under 35 U.S.C. 101 because the claimed

invention is directed to non-statutory subject matter.

-     Regarding Claims 1, 14, and 15,

The claimed invention is not directed to a practical application because

claims 1, 14, and 15 do not require any physical transformation and the invention

as claimed does not produce a useful, concrete, and tangible result.

The claims should be amended to include such practical application as is

supported by the original disclosure, such as transmission of the packet after

processing based upon the test results from the program modules.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35

U.S.C. 102 that form the basis for the rejections under this section made in this

Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4.   Claims 1, 4, 5, 10-15, 18-19, 24-27 are rejected under 35 U.S.C. 102(e) as

being anticipated by Carr et al. (U.S. Patent No. 6,600,744).

        Regarding Claim 1, Carr et al. discloses a method for classifying a data packet

in a network interface, comprising the steps of: (a) receiving a plurality of

classification parameters (Fig.1, Fig. 3, Fig. 4; col 4, lines 2-6. The key

generation block 20 receives the packet 10, or at least the relevant header

information for the packet, and extracts fields from the header to generate the

key. Various portions of various fields may be used to generate the key that is

appropriate for the particular classification operation. The key from the relevant

header of the packet received corresponds to receiving a plurality of classification

parameters);

(b) generating a plurality of program modules, each of said plurality of program

modules for testing for adherence to at least one corresponding classification

parameter (Fig.1, Fig. 3, Fig. 4; col 2, lines 31-36. The rules or parameters for

classifying the packets are stored in a memory structure. The memory structure

receives a set of rule selection signals, and provides a selected set of rules to a

comparison block in response to the rule selection signals. The comparison block also

receives a key that includes the relevant information for classifying the packet

according to the rule set stored in the memory. The rules corresponds to a plurality of

program modules and the comparison block which receives a key that includes the

relevant information for classifying the packet according to the rule is associated with

plurality of program modules for testing for adherence to at least one corresponding

classification parameter);

(c) receiving the data packet (Fig.1, Fig. 3, Fig. 4; col 4, lines 2-6. The key

generation block 20 receives the packet 10, or at least the relevant header

information for the packet, and extracts fields from the header to generate the

key. Various portions of various fields may be used to generate the key that is

appropriate for the particular classification operation. Receiving data packet is

shown in Fig.1, element 10);

(d) generating a header, said header indicating whether one or more predefined

fields are present in the data packet and identifying a location of said one or

more redefined fields in the data packet when present (Fig.1, Fig. 3, Fig. 4; col 1,

lines 42-50; col 3, line 43 through col 4, line 6). Key 24 and the rule selection

signals 22 are generated by a key generation block 20. The key generation block

20 receives the packet 10, or at least the relevant header information for the

packet, and extracts fields from the header to generate the key. Various portions

of various fields may be used to generate the key that is appropriate for the

particular classification operation. As stated earlier, the rule selection signals 22

may be determined based on a number of different factors related to the packet.

The key generation block 20 which extracts fields from the header to generate the key

is associated with generating a header, header indicating whether one or more

predefined fields are present in the data packet and identifying a location of one or more

redefined fields in the data packet when present);

(e) executing each of said plurality of program modules, wherein each of said

plurality of program modules receives said header and generates a test result based

on contents of said header and contents of the data packet (Fig.1, Fig. 3, Fig. 4;

col 2, lines 38-43. The comparison block compares the key to each of the rules in

the selected set of rules, and when a favorable comparison is determined, the

comparison block provides an indication of the favorable comparison is

associated with executing each of plurality of program modules, wherein each of

plurality of program modules receives header and generates a test result based

on contents of header and contents of the data packet. Note: The contents of

header and contents of data packet are inherently considered to be the entire

packet received (element 10)); and

(f) processing the data packet based on said test results from said plurality of

program modules (Fig.1, Fig. 3, Fig. 4; col 2, lines 43-48. A prioritization block

operably coupled to the comparison block prioritizes the rules that resulted in

favorable comparisons to determine a preferred rule, where the preferred rule

includes the resulting classification information for the packet is associated with

processing the data packet based on test results from plurality of program

modules).

Regarding Claim 4, Carr et al. discloses wherein step (f) comprises

transmitting the data packet over a selected service flow based on said test results

from said plurality of program modules (col 4, lines 5-13. The packet classification

engine can be structured such that multiple matches between the key and the rule

set are determined for each key value. Thus, one class of rules may be utilized to

determine the billing class for a packet, whereas another class of rules may be used

to determine the forwarding characteristics for the packet which correspond to

transmitting the data packet over a selected service flow based on said test results

from plurality of program modules).

Regarding Claim 5, Carr et al. discloses wherein step (f) comprises rejecting

the data packet for violating classification parameters based on said test results

from said plurality of program modules (col 4, lines 31-54. When the rules are

used for comparison with the key 24, and a rule is determined as the preferable

rule, the result data corresponding to that rule is included in the output of the

packet classification engine. For example, if a packet is classified based on its

destination address, the results of a favorable comparison with a rule in the

memory array 40 may be to allow the data communication packet to pass

through the switch making decisions based on the packet classification which

can be associated with an unfavorable comparison comprises rejecting the

data packet for violating classification parameters based on test results from

plurality of program modules).

Regarding Claim 10, Carr et al. discloses wherein said steps (a) and (b) occur

during generation of a new service flow (col 8, line 65 through col 9, line 17. When

using a time of day parameter in determining whether or not certain data packets

should be passed. For example, during business hours a particular user may not be

allowed to receive data packets from a particular source. However, when business

hours are over, the lookup table could be updated to point to a new set of rules that

allow for such data packets to be passed. As such, data packets associated with a

specific source or specific protocol may be disallowed during certain times of day,

and allowed during other times of day are associated with steps (a) and (b) occurring

during generation of a new service flow).

Regarding Claim 11, Carr et al. discloses wherein said header is

concatenated to the data packet (Fig. 1 element 10; col 1, lines 42-46. Note: It is

inherent that the data packet contains header and payload fields. Therefore, a header

is inherently concatenated to the payload forming a data packet).

Regarding Claim 12, Carr et al. discloses wherein step (e) comprises

executing each of said plurality of program modules in parallel (col 2, lines 49-56.

Implementing the packet classification engine using a memory that stores many

rules and provides a large number of these rules to the comparison block in

parallel, many rules can be

compared with the key simultaneously is associated with executing each of said

plurality of program modules in parallel).

Regarding Claim 13, Carr et al. discloses wherein step (f) comprises the steps

of: combining said test results from said plurality of program modules using a logical

AND operation (Fig. 2; col 7, lines 61-64. The outputs of all of the comparators are

combined by the AND gate 120 such that all of the comparators must determine a

favorable result to produce a match. 122 between the key 24 and the rule 42 are

associated with combining test results from plurality of program modules using a

logical AND operation); and processing the data packet based on a result of said

logical AND operation (col 8, lines 11-20).

Regarding Claim 14, Carr et al. discloses a method for classifying a data

packet in a network interface, comprising the steps of: (a) receiving a plurality of

classification parameters (Fig.1, Fig. 3, Fig. 4; col 4, lines 2-6. The key generation

block 20 receives the packet 10, or at least the relevant header information for the

packet, and extracts

fields from the header to generate the key. Various portions of various fields

may be used to generate the key that is appropriate for the particular

classification operation. The key from the relevant header of the packet

received corresponds to receiving a plurality of classification parameters);

(b) generating a plurality of optimized program modules, each of said plurality

of program modules for testing for adherence to at least one corresponding

classification parameter (Fig.1, Fig. 3, Fig. 4; col 2, lines 31-36. The rules or parameters for classifying the packets are stored in a memory structure. The memory structure receives a set of rule selection signals, and provides a selected set of rules to a comparison block in response to the rule selection signals. The comparison block also receives a key that includes the relevant information for classifying the packet according to the rule set stored in the memory. The rules corresponds to a plurality of program modules and the comparison block which receives a key that includes the relevant information for classifying the packet according to the rule is associated with plurality of program modules for testing for adherence to at least one corresponding classification parameter);

(c) receiving the data packet (Fig.1, Fig. 3, Fig. 4; col 4, lines 2-6. The key generation block 20 receives the packet 10, or at least the relevant header information for the packet, and extracts fields from the header to generate the key. Various portions of various fields may be used to generate the key that is appropriate for the particular classification operation, Receiving data packet is shown in Fig.1, element 10);

(d) generating a header, said header indicating whether one or more predefined fields are present in the data packet and identifying a location of said one or more predefined fields in the data packet when present (Fig.1, Fig. 3, Fig. 4; col 1, lines 42-50; col 3, line 43 through col 4, line 6. Key 24 and the rule selection signals 22 are generated by a key generation block 20. The key generation block 20 receives the packet 10, or at least the relevant header information for the packet, and extracts fields from the header to

generate the key. Various portions of various fields may be used to generate the key that is appropriate for the particular classification operation. As stated earlier, the rule selection signals 22 may be determined based on a number of different factors related to the packet. The key generation block 20 which extracts fields from the header to generate the key is associated with generating a header, header indicating whether one or more predefined fields are present in the data packet and identifying a location of one or more redefined fields in the data packet when present);

(e) serially executing said plurality of program modules, wherein each of said plurality of program modules receives said header and generates a test result based on contents of. said header and contents of the data packet used to generate the header, until one of said plurality of program modules generates a failing test result (Fig.1, Fig. 3, Fig. 4; col 2, lines 38-43; col 11, line 29 through col 12, line 8; col 13, line 67 through col 14, lines 8. The comparison block compares the key to each of the rules in the selected set of rules, and when a favorable comparison is determined, the comparison block provides an indication of the favorable comparison is associated with executing each of plurality of program modules, wherein each of plurality of program modules receives header and generates a test result based on contents of header and contents of the data packet. The sequencer 250 receives indications from the scheduler 240 that a new key has been received and is to be compared with a certain rule set. The sequencer passes the start index to the lookup table 272 to select the first address offset that is passed to the data array 290. Sequencer 250 correspond to

serially executing plurality of program modules. Fig. 4, step 422. If the linked

list is no longer supplying additional address offsets to retrieve additional rule

sets, the system may return a value indicating that no match has been

achieved and this corresponds to plurality of program modules generates a

failing test result Note: The contents of header and contents of data packet

are inherently considered to be the entire packet received (element 10)); and

(f) processing the data packet based on whether a failing test result was

generated in step (e) (Fig.1, Fig. 3, Fig. 4; col 2, lines 43-48; col 14, lines 8-

15. A prioritization block operably coupled to the comparison block prioritizes

the rules that resulted in favorable comparisons to determine a preferred

rule, where the preferred rule includes the resulting classification information

for the packet is associated with processing the data packet based on test

results from plurality of program modules).

Regarding Claim 15, Carr et al. discloses a method for classifying a data

packet in a network interface, comprising the steps of: (a) receiving a plurality of

classification parameters (Fig.1, Fig. 3, Fig. 4; col 4, lines 2-6. The key generation

block 20 receives the packet 10, or at least the relevant header information for the

packet, and extracts fields from the header to generate the key. Various portions of

various fields may be used to generate the key that is appropriate for the particular

classification operation. The key from the relevant header of the packet received

corresponds to receiving a plurality of classification parameters);

(b) generating a plurality of program modules, each of said plurality of program

modules for testing for adherence to at least one corresponding classification

parameter (Fig.1, Fig. 3, Fig. 4; col 2, lines 31-36. The rules or parameters for

classifying the packets are stored in a memory structure. The memory structure

receives a set of rule selection signals, and provides a selected set of rules to a

comparison block in response to the rule selection signals. The comparison

block also receives a key that includes the relevant information for classifying

the packet according to the rule set stored in the memory. The rules

corresponds to a plurality of program modules and the comparison block which

receives a key that includes the relevant information for classifying the packet

according to the rule is associated with plurality of program modules for testing

for adherence to at least one corresponding classification parameter);

(c) receiving the data packet (Fig.1, Fig. 3, Fig. 4; col 4, lines 2-6. The key

generation block 20 receives the packet 10, or at least the relevant header

information for the packet, and extracts fields from the header to generate the

key. Various portions of various fields may be used to generate the key that is

appropriate for the particular classification operation. Receiving data packet is

shown in Fig.1, element 10);

(d) executing each of said plurality of program modules, wherein each of said

plurality of program modules generates a test result based on contents of the data

packet (Fig.1, Fig. 3, Fig. 4; col 2, lines 38-43. The comparison block compares the

key to each of the rules in the selected set of rules, and when a favorable comparison

is determined, the comparison block provides an indication of the favorable

comparison is associated with executing each of said plurality of program modules,

wherein each of plurality of program modules generates a test result based on

contents of the data packet Note: The contents of data packet are inherently

considered to be the entire packet received (element 10) including the header); and

(e) processing the data packet based on said test results from said plurality of

program modules (Fig.1, Fig. 3, Fig. 4; col 2, lines 43-48. A prioritization block

operably coupled to the comparison block prioritizes the rules that resulted in

favorable comparisons to determine a preferred rule, where the preferred rule

includes the resulting classification information for the packet is associated with

processing the data packet based on test. results from plurality of program modules).

Regarding Claim 18, Carr et al. discloses wherein step (e) comprises

transmitting the data packet over a selected service flow based on said test results

from said plurality of program modules (col 4, lines 5-13. The packet classification

engine can be structured such that multiple matches between the key and the rule

set are determined for each key value. Thus, one class of rules may be utilized to

determine the billing class for a packet, whereas another class of rules may be used

to determine the forwarding characteristics for the packet which correspond to

transmitting the data packet Over a selected service flow based on said test results

from plurality of program modules).

Regarding Claim 19, Carr et al. discloses wherein step (e) comprises

rejecting the data packet for violating classification parameters based on said test

results from said plurality of program modules (col 4, lines 31-54. When the rules

are used for comparison with the key 24, and a rule is determined as the preferable

rule, the result data corresponding to that rule is included in the output of the packet

classification engine. For example, if a packet is classified based on its destination

address, the results of a favorable comparison with a rule in the memory array 40

may be to allow the data communication packet to pass through the switch making

decisions based on the packet classification which can be associated with an

unfavorable comparison 'comprises rejecting the data packet for violating

classification parameters based on test results from plurality of program modules).

Regarding Claim 24, Carr et al. discloses wherein said steps (a) and (b)

occur during generation of a new service flow (col 8, line 65 through col 9, line 17.

When using a time of day parameter in determining whether or not certain data

packets should be passed. For example, during business hours a particular user

may not be allowed to receive data packets from a particular source. However, when

business hours are over, the lookup table could be updated to point to a new set of

rules that allow for such data packets to be passed. As such, data packets

associated with a specific source or specific protocol may be disallowed during

certain times of day, and allowed during other times of day are associated with steps

(a) and (b) occurring during generation of a new service flow).

Regarding Claim 25, Carr et al. discloses wherein step (d) comprises the step

of: executing each of said plurality of program modules in parallel (col 2, lines 49-56.

Implementing the packet classification engine using a memory that stores many

rules and provides a large number of these rules to the comparison block in parallel,

many rules can be compared with the key simultaneously is associated with

executing each of said plurality of program modules in parallel).

Regarding Claim 26, Carr et al. discloses wherein step (e) comprises the

steps of: (1) combining said test results from said plurality of program modules using

a logical AND operation (Fig. 2; col 7, lines 61-64. The outputs of all of the

comparators are combined by the AND gate 120 such that all of the comparators

must determine a favorable result to produce a match 122 between the key 24 and

the rule 42. are associated with combining test results from plurality of program

modules using a logical AND operation); and (2) processing the data packet based

on a result of said logical AND operation (col 8, lines 11-20).

Regarding Claim 27, Carr et al. discloses a computer program product

comprising a computer usable medium having computer program logic for

enabling a processor in a network interface to classify a data packet (col 2, lines

57-66. The packet classification engine may be implemented using dynamic

random access memory (DRAM) technology. The rule set stored within the

memory structure may be modified through a simple memory access that alters

the specific rules within memory. Additionally, the signals utilized to select the

set of rules for a particular comparison can be mapped to different locations

within the memory structure, thus allowing different sets of rules to be utilized in

different sets of conditions. Similarly, the mapping of the rule selection signals to

a specific set of rules is flexible enough that a plurality of different rule sets can

be included in the memory structure, allowing a variety of protocols to be

supported in a single packet classification engine. Note: Dynamic random

access memory (DRAM) technology and the signals utilized to select the set of

rules are inherently associated with a computer program product comprising a

computer usable medium having computer program logic for enabling a

processor in a network interface to classify a data packet) comprising: a first

means for enabling the processor to receive a plurality of classification

parameters (Fig.1, Fig. 3, Fig. 4; col 4, lines 2-6. The key generation block 20

receives the packet 10, or at least the relevant header information for the packet,

and extracts fields from the header to generate the key. Various portions of

various fields may be used to generate the key that is appropriate for the

particular classification operation. The key from the relevant header of the

packet received corresponds to receiving a plurality of classification

parameters); a second means for enabling the processor to generate a plurality

of program modules, each of said plurality of program modules for testing for

adherence to at least one corresponding classification parameter (Fig.1, Fig. 3,

Fig. 4; col 2, lines 31-36). The rules or parameters for classifying the packets are

stored in a memory structure. The memory structure receives a set of rule selection

signals, and provides a selected set of rules to a comparison block in response to the

rule selection signals. The comparison block also receives a key that includes the

relevant information for classifying the packet according to the rule set stored in the

memory. The rules corresponds to a plurality of program modules and the

comparison block which receives a key that includes the relevant information for

classifying the packet according to the rule is associated with plurality of program

modules for testing for adherence to at least one corresponding classification

parameter);

a third means for enabling the processor to receive the data packet (Fig.1, Fig. 3, Fig.

4; col 4, lines 2-6. The key generation block 20 receives the packet 10, or at

least the relevant header information for the packet, and extracts fields from the

header to generate the key. Various portions of various fields may be used to

generate the key that is appropriate for the particular classification operation.

Receiving data packet is shown in Fig.1, element 10);

a fourth means for enabling the processor to generate a header, said header

indicating whether one or more predefined fields are present in the data packet

and identifying a location of said one or more predefined fields of the data

packet when present (Fig.1, Fig. 3, Fig. 4; col 1, lines 42-50; col 3, line 43

through col 4, line 6). Key 24 and the rule selection signals 22 are generated by

a key generation block 20. The key generation block 20 receives the packet 10,

or at least the relevant header information for the packet, and extracts fields from

the header to generate the key. Various portions of various fields may be used

to generate the key that is appropriate for the particular classification operation.

As stated earlier, the rule selection signals 22 may be determined based on a number of different factors related to the packet. The key generation block 20 which extracts fields from the header to generate the key is associated with generating a header, header indicating whether one or more predefined fields are present in the data packet and identifying a location of one or more redefined fields in the data packet when present);

a fifth means for enabling the processor to execute each of said plurality of program modules, wherein each of said plurality of program modules receives said header and generates a test result based on contents of said header and contents of said data packet (Fig.1, Fig. 3, Fig. 4; col 2, lines 38-43. The comparison block compares the key to each of the rules in the selected set of rules, and when a favorable comparison is determined, the comparison block provides an indication of the favorable comparison is associated with executing each of plurality of program modules, wherein each of plurality of program modules receives header and generates a test result based on contents of header and contents of the data packet. Note: The contents of header and contents of data packet are inherently considered to be the entire packet received (element 10)); and

a sixth means for enabling the processor to process the data packet based on said test results from said plurality of program modules (Fig.1, Fig. 3, Fig. 4; col 2, lines 43-48. A prioritization block operably coupled to the comparison block prioritizes

the rules that resulted in favorable comparisons to determine a preferred rule,

where the preferred rule includes the resulting classification information for the

packet is associated with processing the data packet based on test results from

plurality of program modules).

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described
> as set forth in section 102 of this title, if the differences between the subject matter sought to
> be patented and the prior art are such that the subject matter as a whole would have been
> obvious at the time the invention was made to a person having ordinary skill in the art to which
> said subject matter pertains. Patentability shall not be negatived by the manner in which the
> invention was made.

6.   Claims 2, 6-9, 16, 20-23, 28, 30-39 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Carr et al.(U.S. Patent No. 6,600,744) in view of

Synnestvedt et at. (U.S. Patent No. 6,598,057).

Regarding Claim 2, Carr et al. discloses all the limitations of claim 1.

Carr et al. does not disclose wherein said classification parameters comprise

DOCSIS classification parameters.

Synnestvedt et al. discloses classification parameters comprising DOCSIS

classification parameters (Fig. 2, element 206; col 3, lines 44-48; col 4, lines 8-20).

At the time the invention was made it would have been obvious to a person of

ordinary skill in the art to include the DOCSIS classification parameters as taught by

Synnestvedt et al. into the classification system of Carr et al. allowing for more effective

broadband provisioning through better configuration file management as well as

allowing for the creation of more flexible subscriber service plans wherein the

resulting configuration can be generated according to the DOCSIS configuration file

standard (col 2, lines 63-65; col 3, lines 9-12).

Regarding Claim 6, Carr et al. discloses all the limitations of claim 1. Carr et

at. does not disclose wherein step (a) comprises receiving a configuration file,

said configuration file including said plurality of classification parameters.

Synnestvedt et al. discloses wherein step (a) comprises receiving a

configuration file, said configuration file including said plurality of classification

parameters (Fig. 2; col 4, lines 9-20. The DOCSISFile class 206 inherits from

DynamicFile class 204, and represents a DOCSIS compliant configuration file

which corresponds to receiving a configuration file, configuration file including

plurality of classification parameters). At the time the invention was made it

would have been obvious to a person of ordinary skill in the art to include the

DOCSIS classification parameters as taught by Synnestvedt et al. into the

classification system of Carr et al. allowing for more effective broadband

provisioning through better configuration file management as well as allowing

for the creation of more flexible subscriber service plans wherein the resulting

configuration can be generated according to the DOCSIS configuration file

standard (col 2, lines 63-65; col 3, lines 9-12).

Regarding Claim 7, Carr et al. discloses all the limitations of claim 1.

Carr et al. does not disclose wherein step (a) comprises receiving a cable

modem configuration request, said cable modem configuration request including

said plurality of classification parameters. Synnestvedt et al. discloses wherein

step (a) comprises receiving a cable modem configuration request, said cable

modem configuration request including said plurality of classification

parameters (Fig. 1; col 3, lines 44-48; col 4, lines 5-8). Requests for

configuration originate at cable modem 102 and travel to TFTP (Trivial File

Transfer Protocol) server 124, where a DOCSIS binary configuration file is

generated and sent back to cable modem correspond to receiving a cable

modem configuration request, cable modem configuration request including

plurality of classification parameters). At the time the invention was made it

would have been obvious to a person of ordinary skill in the art to include the

DOCSIS classification parameters as taught by Synnestvedt et al. into the

classification system of Carr et al. allowing for more effective broadband

provisioning through better configuration file management as well as allowing

for the creation of more flexible subscriber service plans wherein the resulting

configuration can be generated according to the DOCSIS configuration file

standard (col 2, lines 63-65; col 3, lines 9-12).

Regarding Claim 8, Carr et al. discloses all the limitations of claim 1. Carr et

al. does not disclose wherein step (a) comprises receiving a dynamic service

message, wherein said dynamic service message includes said plurality of

classification parameters. Synnestvedt et al. discloses wherein step (a) comprises

receiving a dynamic service message, wherein said dynamic service message

includes said plurality of classification parameters (Fig. 4; col 5, lines 11-16. A

DOCSIS configuration file is dynamically generated based upon a RRQ message

received by an augmented TFTP (Trivial File Transfer Protocol) server 124 is

associated with receiving a dynamic service message, wherein dynamic service

message includes plurality of classification parameters). At the time the invention

was made it would have been obvious to a person of ordinary skill in the art to

include the DOCSIS classification parameters as taught by Synnestvedt et al. into

the classification system of Carr et al. allowing for more effective broadband

provisioning through better configuration file management as well as allowing for the

creation of more flexible subscriber service plans wherein the resulting configuration

can be generated according to the DOCSIS configuration file standard (col 2, lines

63-65; col 3, lines 9-12).

Regarding Claim 9, Carr et al. discloses all the limitations of claim 1.

Carr et al. does not disclose wherein said steps (a) and (b) occur as part of a

cable modem registration process. Synnestvedt et al. discloses wherein said

steps (a) and (b) occur as part of a cable modem registration process (Fig. 4,

steps 416, 418 and 420; col 3, lines 44-48; col 10, lines 16-18. Steps 416, 418

and 420 correspond to steps (a) and (b) occuring as part of a cable modem

registration process). At the time the invention was made it would have been

obvious to a person of ordinary skill in the art to include the DOCSIS

classification parameters as taught by Synnestvedt et al. into the classification

system of Carr et al. allowing for more effective broadband provisioning

through better configuration file management as well as allowing for the

creation of more flexible subscriber service plans wherein the resulting

configuration can be generated according to the DOCSIS configuration file standard

(col 2, lines 63-65; col 3, lines 9-12).

Regarding Claim 16, Carr et al. discloses all the limitations of claim 15. Carr et

at. does not disclose wherein said classification parameters comprise DOCSIS

classification parameters. Synnestvedt et al. discloses classification parameters

comprise DOCSIS classification parameters (Fig. 2, element 206; col 3, lines 44-48;

col 4, lines 8-20). At the time the invention was made it would have been obvious to a

person of ordinary skill in the art to include the DOCSIS classification parameters as

taught by Synnestvedt et al. into the classification system of Carr et al. allowing for

more effective broadband provisioning through better configuration file management as

well as allowing for the creation of more flexible subscriber service plans wherein the

resulting configuration can be generated according to the DOCSIS configuration file

standard (col 2, lines 63-65; col 3, lines 9-12).

Regarding Claim 20, Carr et al. discloses all the limitations of claim 15. Carr et

al. does not disclose wherein step (a) comprises receiving a configuration file, said

configuration file including said plurality of classification parameters. Synnestvedt et

al. discloses wherein step (a) comprises receiving a configuration file, said

configuration file including said plurality of classification parameters (Fig. 2; col 4,

lines 9-20. The DOCSISFile class 206 inherits from DynamicFile class 204, and

represents a DOCSIS compliant configuration file which corresponds to receiving a

configuration file, configuration file including plurality of classification parameters). At

the time the invention was made it would have been obvious to a person of ordinary

skill in the art to include the DOCSIS classification parameters as taught by

Synnestvedt et al. into the classification system of Carr et al. allowing for more

effective broadband provisioning through better configuration file management as

well as allowing for the creation of more flexible subscriber service plans wherein the

resulting configuration can be generated according to the DOCSIS configuration file

standard (col 2, lines 63-65; col 3, lines 9-12).

Regarding Claim 21, Carr et al. discloses all the limitations of claim 15. Carr et

al. does not disclose wherein step (a) comprises receiving a cable modem

configuration request, said cable modem configuration request including said plurality

of classification parameters. Synnestvedt et al. discloses wherein step (a) comprises

receiving a cable modem configuration request, said cable modem configuration

request including said plurality of classification parameters (Fig. 1; col 3, lines 44-48;

col 4, lines 5-8). Requests for configuration originate at cable modem 102 and travel

to TFTP (Trivial File Transfer Protocol) server 124, where a DOCSIS binary

configuration file is generated and sent back to cable modem correspond to receiving

a cable modem configuration request, cable modem configuration request including

plurality of classification parameters). At the time the invention was made it would

have been obvious to a person of ordinary skill in the art to include the DOCSIS

classification parameters as taught by Synnestvedt et al. into the classification

system of Carr et al. allowing for more effective broadband provisioning through

better configuration file management as well as allowing for the creation of more

flexible subscriber service plans wherein the resulting configuration can be generated

according to the DOCSIS configuration file standard (col 2, lines 63-65; col 3, lines 9-

12).

Regarding Claim 22, Carr et al. discloses all the limitations of claim 15.

Carr et at. does not disclose wherein step (a) comprises receiving a dynamic

service message, wherein said dynamic service message includes said plurality

of classification parameters. Synnestvedt et al. discloses wherein step (a)

comprises receiving a dynamic service message, wherein said dynamic service

message includes said plurality of classification parameters (Fig. 4; col 5, lines 11-16.

A DOCSIS configuration file is dynamically generated based upon a RRQ message

received by an augmented TFTP (Trivial File Transfer Protocol) server 124 is

associated with receiving a dynamic service message, wherein dynamic service

message includes plurality of classification parameters). At the time the invention was made it would have been obvious to a person of ordinary skill in the art to include the DOCSIS classification parameters as taught by Synnestvedt et al. into the classification system of Carr et al. allowing for more effective broadband provisioning through better configuration file management as well as allowing for the creation of more flexible subscriber service plans wherein the resulting configuration can be generated according to the DOCSIS configuration file standard (col 2, lines 63-65; col 3, lines 9-12).

Regarding Claim 23, Carr et al. discloses all the limitations of claim 15. Carr et al. does not disclose wherein said steps (a) and (b) occur as part of a cable modem registration process. Synnestvedt et al. discloses wherein said steps (a) and (b) occur as part of a cable modem registration process (Fig. 4, steps 416, 418 and 420; col 3, lines 44-48; col 10, lines 16-18. Steps 416, 418 and 420 correspond to steps (a) and (b) occuring as part of a cable modem registration process). At the time the invention was made it would have been obvious to a person of ordinary skill in the art to include the DOCSIS classification parameters as taught by Synnestvedt et al. into the classification system of Carr et al. allowing for more effective broadband provisioning through better configuration file management as well as allowing for the creation of

more flexible subscriber service plans wherein the resulting configuration can be

generated according to the DOCSIS configuration file standard (col 2, lines 63-65; col

3, lines 9-12).

Regarding Claim 28, Carr et al. discloses all the limitations of claim 27. Carr et

al. does not disclose wherein said classification parameters comprise DOCSIS

classification parameters. Synnestvedt et al. discloses classification parameters

comprise DOCSIS classification parameters (Fig. 2, element 206; col 3, lines 44-48;

col 4, linesl 8-20). At the time the invention was made it would have been obvious to

a person of ordinary skill in the art to include the DOCSIS classification parameters

as taught by Synnestvedt et al. into the classification system of Carr et al. allowing for

more effective broadband provisioning through better configuration file management

as well as allowing for the creation of more flexible subscriber service plans wherein

the resulting configuration can be generated according to the DOCSIS configuration

file standard (col 2; lines 63-65; col 3, lines 9-12).

Regarding Claim 30, Carr et al. and Synnestvedt et al. discloses all the

limitations of claims 27 and 28. Further Carr et al. discloses wherein said sixth

means comprises means for enabling the processor to transmit the data packet over a

selected service flow based on said test results from said plurality of program

modules (col 4, lines 5-13. The packet classification engine can be structured such

that multiple matches between the key and the rule set are determined for each key

value. Thus, one class of rules may be utilized to determine the billing class for a

packet, whereas another class of rules may be used to determine the forwarding

characteristics for the packet which correspond to enabling the processor to transmit

the data packet over a selected service flow based on said test results from said

plurality of program modules).

Regarding Claim 31, Carr et al. and Synnestvedt et at. discloses all the

limitations of claims 27 and 28. Further Carr et at. discloses wherein said sixth means

comprises means for enabling the processor to reject the data packet for violating

classification parameters based on said test results from said plurality of program

modules (col 4, lines 31-54. When the rules are used for comparison with the key 24,

and a rule is determined as the preferable rule, the result data corresponding to that

rule is included in the output of the packet classification engine. For example, if a

packet is classified based on its destination address, the results of a favorable

comparison with a rule in the memory array 40 may be to allow the data

communication packet to pass through the switch making decisions based on the

packet classification which can be associated with an unfavorable comparison comprises rejecting the data packet for violating classification parameters based on test results from plurality of program modules).

Regarding Claim 32, Carr et al. and Synnestvedt et al. discloses all the limitations of claims 27 and 28. Further Synnestvedt et at. discloses wherein said first means comprises means for enabling the processor to receive a plurality of classification parameters retrieved from a configuration file (Fig. 2; col 4, lines 9-20. The DOCSISFile class 206 inherits from DynamicFile class 204, and represents a DOCSIS compliant configuration file which corresponds to enabling the processor to receive a plurality of classification parameters retrieved from a configuration file).

Regarding Claim 33, Carr et al. and Synnestvedt et al. discloses all the limitations of claims 27 and 28. Further Synnestvedt et al. discloses wherein said first means comprises means for enabling the processor to receive a plurality of classification parameters retrieved from a cable modem configuration request (Fig. 1; col 3, lines 44-48; col 4, lines 5-8. Requests for configuration originate at cable modem 102 and travel to TFTP (Trivial File Transfer Protocol) server 124, where a DOCSIS binary configuration file is generated and sent back to cable modem correspond to enabling the processor to receive a plurality of classification parameters retrieved from a cable modem configuration request).

Regarding Claim 34, Carr et at. and Synnestvedt et at. discloses all the

limitations of claims 27 and 28. Further Synnestvedt et al. discloses wherein said first

means comprises means for enabling the processor to receive a plurality of

classification parameters retrieved from a dynamic service message (Fig. 4; col 5,

lines 11-16. A DOCSIS configuration file is dynamically generated based upon a

RRQ message received by an augmented TFTP (Trivial File Transfer Protocol)

server 124 is associated with enabling the processor to receive a plurality of

classification parameters retrieved from a dynamic service message).

Regarding Claim 35, Carr et al. and Synnestvedt et al. discloses all the

limitations of claims 27 and 28. Further Synnestvedt et al. discloses wherein said

first means and said second means are executed as part of a cable modem

registration request (Fig. 4, steps 416, 418 and 420; col 3, lines 44-48; col 10, lines

16-18. Steps 416, 418 and 420 correspond to steps (a) and (b) occurring as part

of a cable modem registration request).

Regarding Claim 36, Carr et al. and Synnestvedt et al. discloses all the

limitations of claims 27 and 28. Further Carr et al. discloses wherein said first

means and said second means are executed during generation of a new

service flow (col 8, line 65 through col 9, line 17. When using a time of day

parameter in determining whether or not certain data packets should be

passed. For example, during business hours a particular user may not be

allowed to receive data packets from a particular source. However, when

business hours are over, the lookup table could be updated to point to a new

set of rules that allow for such data packets to be passed. As such, data

packets associated with a specific source or specific protocol may be

disallowed during certain times of day, and allowed during other times of day

are associated with first means and second means executed during generation

of a new service flow).

Regarding Claim 37, Carr et al. and Synnestvedt et al. discloses all the

limitations of claims 27 and 28. Further Carr et al. discloses wherein said fourth

means comprises means for enabling the processor to concatenate said header

to the data packet (Fig. 1 element 10; col 1, lines 42-46. Note: It is inherent that

the data packet contains header and payload fields. Therefore, a header is

inherently concatenated to the payload forming a data packet).

Regarding Claim 38, Carr et al. and Synnestvedt et al. discloses all the

limitations of claims 27 and 28. Further Carr et al. discloses wherein said fifth

means comprises means for enabling the processor to execute each of said

plurality of program modules in parallel (col 2, lines 49-56. Implementing the

packet classification engine using a memory that stores many rules and

provides a large number of these rules to the comparison block in parallel,

many rules can be compared with the key simultaneously is associated with

enabling the processor to execute each of plurality of program modules in parallel).

Regarding Claim 39, Carr et al. and Synnestvedt et al. discloses all the limitations of claims 27 and 28. Further Carr et al. discloses wherein said sixth means comprises means for enabling the processor to combine said test results from said plurality of program modules using a logical AND operation and process the data packet based on a result of said logical AND operation (Fig. 2; col 7, lines 61-64. The outputs of all of the comparators are combined by the AND gate 120 such that all of the comparators must determine a favorable result to produce a match 122 between the key 24 and the rule 42. are associated with combining test results from plurality of program modules using a logical AND operation. Col 8, lines 11-20 is associated with processing the data packet based on a result of said logical AND operation).

7.   Claims 3, 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carr et al. (U.S. Patent No. 6,600,744) in view of Connery et al. (U.S. Patent No. 6,570,884).

Regarding Claim 3, Carr et al. discloses all the limitations of claim 1. Carr

et al. does not disclose wherein step (f) comprises applying packet header

suppression to the data packet based on said test results from said plurality of

program modules. Connery et al. discloses wherein step (f) comprises applying

packet header suppression to the data packet based on said test results from

said plurality of program modules. (col 8, lines 53-57. For the pattern matching

engines to have an optional capability to treat an incoming SNAP encapsulated

IP packet as if it were an EtherType encapsulation. For this type of packet, the

SNAP header is ignored in the pattern matching process. Ignoring the SNAP

header in the pattern matching process is associated with packet header

suppression to the data packet based on test results from plurality of program

modules). At the time the invention was made it would have been obvious to a

person of ordinary skill in the art to apply the teachings of Connery et al. into the

system of Carr et al. such that the processor is only required to handle packet

identified by the dedicated packet filter logic, it need not have the capability to

keep up with the entire data stream (col 2, lines 13-16).

Regarding Claim 17, Carr et al. discloses all the limitations of claim 15. Carr

et al. does not disclose wherein step (e) comprises applying packet header

suppression to the data packet based on said test results from said plurality of

program modules. Connery et al. discloses wherein step (e) comprises applying

packet header suppression to the data packet based on said-test results from said

plurality of program modules. (col 8, lines 53-57. For the pattern matching engines to

have an optional capability to treat an incoming SNAP encapsulated IP packet as if it

were an EtherType encapsulation. For this type of packet, the SNAP header is

ignored in the pattern matching process. Ignoring the SNAP header in the pattern

matching process is associated with packet header suppression to the data packet

based on test results from plurality of program modules). At the time the invention

was made it would have been obvious to a person of ordinary skill in the art to apply

the teachings of Connery et al. into the system of Carr et al. such that the processor

is only required to handle packets identified by the dedicated packet filter logic, it

need not have the capability to keep up with the entire data stream (col 2, lines 13-

16).

8.   Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Carr

et al.(U.S. Patent No. 6,600,744) in view of Synnestvedt et at. (U.S. Patent No.

6,598,057) and further in view of Connery et al. (U.S. Patent No. 6,570,884).

        Regarding Claim 29, Carr et al. and Synnestvedt et al. discloses all the

limitations of claims 27 and 28. Carr et al. and Synnestvedt et al. does not disclose

wherein said sixth means comprises means for enabling the processor to apply

packet header suppression to the data packet based on said test results from said

plurality of program modules. Connery et al. discloses wherein said sixth means

comprises means for enabling the processor to apply packet header suppression to

the data packet based on said test results from said plurality of program modules.

(col 8, lines 53-57. For the pattern matching engines to have an optional capability to

treat an incoming SNAP encapsulated IP packet as if it were an EtherType

encapsulation. For this type of packet, the SNAP header is ignored in the pattern

matching process. Ignoring the SNAP header in the pattern matching process is

associated with packet header suppression to the data packet based on test results

from plurality of program modules). At the time the invention was made it would have

been obvious to a person of ordinary skill in the art to apply the teachings of Connery

et al. into the system of Carr et al. and Synnestvedt et al. such that the processor is

only required to handle packets identified by the dedicated packet filter logic, it need

not have the capability to keep up with the entire data stream (col 2, lines 13-16).

Response to Arguments

9.   Applicant's arguments filed 11/15/2006 have been fully considered but
they are not persuasive.

- On pgs. 1-5 of the Pre-Appeal Brief Request, Applicant contends

   that Carr does not disclose generating a plurality of program

   modules to test for adherence to at least one corresponding

   classification parameter. Applicant argues that the stored

   rules/parameters and their subsequent use by comparison block 50

   in Carr does not meet the claimed "program modules" because

Carr discloses the various testing operations performed at
comparison block 50 are preferably implemented in hardware,
whereas the claimed "program modules" claimed by Applicant are
implemented in software.

- In response to applicant's argument that the references fail to show
certain features of applicant's invention, it is noted that the features
upon which applicant relies (software versus hardware
implementation as well as the modification and re-ordering of
testing operations) are not recited in the rejected claim(s).
Although the claims are interpreted in light of the specification,
limitations from the specification are not read into the claims. See
In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir.
1993). Furthermore, as shown in the Advisory Action filed
10/3/2006, Carr shows that the various components shown in Fig. 3
are implemented through logic on DRAM process, known in the art
to be a software application that meets the disclosure of Applicant's
generated "program modules" (also see the rejection of Claim 27
above, pg. 15-16).

- On pgs. 1-5 of the Pre-Appeal Brief Request, Applicant contends
that Carr does not disclose performing the claim limitations at a
network interface.

- In response to applicant's arguments, the recitation "network interface" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951). However, Carr shows that the disclosed packet processing is based upon examining the headers of the packets at various points in the network (Col. 1, lines 16-18). Therefore, even if the recitation of "network interface" where placed in the body of the claim, it would be met by the disclosure of Carr.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gregory B. Sefcheck whose telephone number is 571-272-3098. The examiner can normally be reached on Monday-Friday, 8:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Seema Rao can be reached on 571-272-3174. The fax

phone number for the organization where this application or proceeding is

assigned is 571-273-8300.

Information regarding the status of an application may be obtained from

the Patent Application Information Retrieval (PAIR) system. Status information

for published applications may be obtained from either Private PAIR or Public

PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free). If you would like assistance from a USPTO Customer Service

Representative or access to the automated information system, call 800-786-

9199 (IN USA OR CANADA) or 571-272-1000.

GBS *GBS*
1-9-2007

SEEMA S. RAO   1/11/07
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600